PETROLEUMSTILSYNET

Forsvarsdepartementet
Postboks 8126 Dep

0032 Oslo

Vår saksbehandler
Hilda Kjeldstad

Deres ref.	Vår ref. (bes oppgitt ved svar)	Dato
2015/3139-254	Ptil 2018/504/hk	28.9.2018

Svar på høring om forskrifter til ny sikkerhetslov

Vi viser til høring av nye forskrifter til sikkerhetsloven. Vi har deltatt i utarbeidelsen av forskriftene, og har avgitt kommentarer underveis i arbeidet. Derfor har vi nå valgt å begrense våre innspill til de områdene hvor departementet spesielt ønsker høringsinstansenes innspill i henhold til høringsnotatet. Kommentarene er listet opp kronologisk i henhold til høringsbrevet, og sidenummer henviser til dette. Skrift i kursiv er gjengivelse fra høringsbrevet.

Side 10: *(...) Departementet ber likevel om høringsinstansenes syn på om det bør fremgå ytterligere momenter i forskriftene, og i så fall hvilke.*

Det etterspørres hvorvidt det er nødvendig/ formålstjenlig å forskriftsfeste momenter som skal vektlegges i vurderingen av hvilke virksomheter loven skal gjelde for. Som tidligere påpekt, er vår vurdering at kriteriene som legges til grunn i loven § 1-5 første ledd nr. 1 bokstav d om hva som menes med nasjonale sikkerhetsinteresser, ikke dekkende for petroleumsvirksomhet. Det vises i denne sammenheng til prop. 153 L side 35 hvor departementet understreker at «det er opp til det enkelte departement innenfor sitt myndighetsområde å avgjøre hvilke virksomheter som er av en slik betydning at de skal underlegges loven.»

Side 11: *De kravene som gjelder for alle virksomhetene som underlegges loven skal sikre et forsvarlig sikkerhetsnivå for informasjon gradert BEGRENSET, for ugradert skjermingsverdig informasjon og skjermingsverdige informasjonssystemer som ikke behandler sikkerhetsgradert informasjon høyere enn BEGRENSET.*

Dette kan bety at infrastruktur og objekter skal være sikret som informasjonssystemer som «ikke behandler sikkerhetsgradert informasjon høyere enn BEGRENSET». Denne tilnærmingen synes å være forankret i at objekter og infrastruktur i basis kan sikres som

gradert informasjon. Dette står i noen grad i kontrast til anmodning om høringsuttalelse på side 13 der den aktuelle tilsynsmyndigheten blir tillagt ansvaret for konkretisering.

Side 11: *Departementet ber om høringsinstansenes innspill på om forslaget til inndelingen i forskrifter er hensiktsmessig, og særlig på om det er mer hensiktsmessig med en eller to forskrifter. Departementet ber også om innspill til offisielle korttitler på forskriftene for å sikre at de er tilstrekkelig entydige.*

Det synes hensiktsmessig med den tredelte oppdelingen som er foreslått. Forskriftstitlene kunne med fordel være relatert til sikkerhetsloven, for eksempel

- *forskrift om myndigheters roller og ansvar for nasjonal sikkerhet etter sikkerhetsloven (myndighetsforskriften)*
- *forskrift om klarering av leverandører og personell i medhold av sikkerhetsloven (klareringsforskriften)*
- *forskrift om virksomhet underlagt sikkerhetsloven sitt arbeid med forebyggende sikkerhet (virksomhetsforskriften).*

Side 13: *NSM og sektormyndighetene med tilsynsansvar, vil derfor ha en viktig rolle med å gi råd og veiledning om hvordan bestemmelsene kan etterleves og hvordan tiltakene kan tilpasses en sektors egenart.*

Denne problemstillingen er i noen grad diskutert i neste punkt. Formuleringen slik den framkommer i høringsnotatet kan imidlertid være utfordrende da dette kan bety at NSM og sektormyndigheter har oversikt over konkrete løsninger som er akseptable. Vår veiledning til næringen er ikke basert på slike spesifikke tilnærminger, men basert på standarder og vår involvering i utarbeidelse og revisjon av disse.

Side 13: *Departementet ber høringsinstansenes syn på om det bør gis mer detaljerte krav til sikring av infrastruktur, og i så fall hvilke krav som bør stilles.*

Detaljerte krav til sikring av infrastruktur vil måtte være spesifikke for de ulike typene infrastrukturer og vil følgelig ha til dels svært ulik karakter. Det er allerede påpekt i høringsnotatet (kapittel 3.4, siste avsnitt) at det er behov for at råd, veiledning og tiltak tilpasses en sektors egenart.

Side 15: *Virksomheten må derfor vurdere hvilke kategorier trusselaktører virksomheten er utsatt for, og hvordan disse kategoriene av trusselaktører normalt vil gjennomføre sikkerhetstruende virksomhet.*

Vi ser at dette tankesettet passer best for målrettede angrep. Sikring mot IKT-relaterte hendelser må også inkludere et fokus på de ikke målrettede truslene. Disse fører til den absolutt største andelen av sikkerhetsbrudd i virksomhetene. Åpen trusselvurdering og NSM sine tiltak for IKT-beskyttelse vil være de viktigste elementene her. Samtidig antar vi at for nye virksomheter som underlegges sikkerhetsloven, vil dette bidra til en forenkling av informasjon om trusselaktører, angrepsvektorer og begrensning av sikkerhetstruende virksomhet.

Side 16: *Videre vil det være aktuelt å avtale hvordan NSM best kan tilrettelegge for at sektor-myndighetene får tilgang på relevant informasjon om trusler og sårbarheter slik at disse kan legges til grunn i sektormyndighetenes tilsyns- og rådgivningsoppgaver.*

Den informasjonsdelingen som i dag er tilgjengelig om sårbarheter når det gjelder IKT-relaterte trusler, både fra NSM om IT-relaterte sårbarheter og fra KraftCERT om sårbarheter innen industrielle systemer, er informasjon som bør gå direkte til den enkelte virksomhet.

Videre er det vanskelig å se for seg at informasjon om trusler og sårbarheter vil ha så lang gyldighet at de er relevante som spesifikke tilsynstema. Det vil her trolig være mer relevant å se på virksomhetenes håndtering og konkretisering av aksjoner i forhold til slik informasjon.

Side 20: *Departementet ber imidlertid om høringsinstansenes innspill på om det er behov for en bestemmelse som konkretiserer vurderingstemaene ytterligere, og vil vurdere en slik bestemmelse i lys av høringsinnspillene.*

Det framgår ikke eksplisitt om betenkningene knyttet til klarering av utenlandske statsborgere også gjelder for adgangsklarering eller bare for sikkerhetsklarering. Nest siste setning i 4.5.2 synes å avklare at det gjelder sikkerhetsklarering.

For petroleumssektoren er det viktig å være klar over at det benyttes en del utenlandsk service-personell med nøkkelkompetanse. Dette er oftest personell som benyttes på kort varsel der det ikke er tid til en prosess for adgangsklarering. Det er grunn til å anta at dette vil måtte håndteres etter loven § 8-3 andre ledd ved at dette personellet gis tilgang til objekter under oppsyn av virksomhetens eget personell.

Side 22: *Departementet ber derfor om høringsinstansenes syn på behovet for og hensiktsmessigheten av den unntaksbestemmelsen som er foreslått i myndighetsforskriften § 11, og vil vurdere bestemmelsen i lys av høringsinnspillene.*

Vi mener at unntaksbestemmelsen bør opprettholdes som foreslått, denne vil også bidra til å løse utfordringer med utenlandsk servicepersonell som nevnt over.

Side 23: *Når det gjelder behovet for kompetanse som Norge ikke har tilstrekkelig tilgang på nasjonalt, antar departementet at denne som utgangspunkt kan anskaffes som en sikkerhetsgradert anskaffelse fra land Norge har et sikkerhetssamarbeid med.*

Vi deler ikke denne antakelsen. Objekter og infrastruktur som er i bruk i dag, og som blir underlagt lovens virkeområde, vil heller ikke nødvendigvis kunne skifte ut tekniske styresystemer med tilsvarende fra andre leverandører med samme spesifikasjoner.

Side 24: *Departementet antar at det vil være mer hensiktsmessig at myndigheter med sektoransvar lager veiledere med momenter som kan vektlegges i vurderingen. Departementet ber om høringsinstansenes innspill på om det er nødvendig med ytterligere forskriftsbestemmelser knyttet til denne bestemmelsen.*

Vi deler departementets antakelse om at det er mest hensiktsmessig at myndigheter med sektoransvar lager veiledere for sin sektor. Dette kan medføre sektorvise forskjeller, men gevinsten ved å være sektorspesifikk vurderes som viktigere.

Side 25: *Departementet ber om høringsinstansenes syn på hvem som bør være klareringsmyndighet for leverandørklarering.*

Det er viktig at klareringsmyndigheten for leveranser til infrastruktur og objekter også har tilstrekkelig kompetanse om denne typen systemer. Vi mener derfor at utgangspunktet bør være at sikkerhetsmyndigheten er klareringsmyndighet, men med bistand fra sektormyndigheten. Dette kan reguleres gjennom samarbeidsavtalen mellom sikkerhetsmyndigheten og sektormyndigheten.

Side 26: *Departementet mener i utgangspunktet at det følger av den alminnelige forvaltningsretten at virksomhetene skal gis rimelig frist for å oppfylle kravene i regelverket. Departementet ser likevel at det kan være hensiktsmessig med en egen bestemmelse som regulerer hvilke momenter som skal vurderes når det settes en konkret frist for at hvert enkelt informasjonssystem, infrastruktur eller objekt oppnår et forsvarlig sikringsnivå. Departementene ber om høringsinstansenes innspill, og vil vurdere en slik bestemmelse i lys av høringsrunden.*

For å gi konkrete frister for å oppnå et forsvarlig sikringsnivå må hver enkel organisasjon, objekt og infrastruktur vurderes i forhold til nåværende sikringsnivå. Vurderingen vil måtte være en kombinasjon av operasjonelle, organisatoriske og tekniske forhold. Som norm for vurderingene vil relevante deler av NSMs veileder i sikkerhetsstyring kunne legges til grunn.

Side 27: *Det legges opp til at sektormyndighetene, på bakgrunn av kunnskap om egen sektor og basert på rådgivning fra NSM, skal legge føringer for hva som er et forsvarlig sikkerhetsnivå.*

Vi støtter denne tilnærmingen.

Side 32: *Departementet ber om høringsinstansenes syn på om ovennevnte kriterier er tilstrekkelige for at departementene skal kunne beslutte et klassifiseringsnivå.*

Vi antar at det vil være fornuftig å utvikle en momentliste for vurdering av hvilke virksomheter loven skal gjelde for. I merknadene til myndighetsforskriften § 1 er det referert til KIKS-modellen, og det er forslått at denne modellen kan tilpasses sikkerhetsloven for å gi departementene tilstrekkelige kriterier for å kunne beslutte klassifiseringsnivå etter loven § 7-1. KIKS-modellen er p.t. utilstrekkelig, men vi støtter forslaget om å tilpasse modellen til sikkerhetslovens formål og virkeområde.

Side 32: *Adgangsklarering er en ny type klarering, jf. sikkerhetsloven § 8-3. Departementet har foreslått å presisere at adgangsklarering kan benyttes som sikkerhetstiltak dersom fysisk eller elektronisk tilgang til hele eller deler av et klassifisert objekt eller infrastruktur gjør det mulig å skade grunnleggende nasjonale funksjoner.*

I loven § 8-3 andre ledd framkommer det at det ikke skal «fattes vedtak om krav til adgangsklarering dersom det kan iverksettes andre egnede sikkerhetstiltak». Vi kan ikke se at denne preferansen av andre tiltak er synliggjort i forskriften eller høringsnotatet.

Side 33: *Departementet ber høringsinstansenes syn på om bestemmelsen gir tilstrekkelige føringer for å benytte tredjeparter til disse oppgavene.*

Det bør inkluderes føringer om kompetanse også om de systemene det utføres undersøkelser på. Aggressiv testing på enkelte objekter og infrastruktur kan medføre tap av funksjon da den primære beskyttelsen av slike systemer er etablert ved skall som ligger utenfor.

Side 34: *6.2.6 Til § 8 Register over avgjørelser om personklarering:* Det synes ikke å framgå om registeret skal omfatte både sikkerhetsklarering og adgangsklarering.

Side 37: *Departementene ber høringsinstansene om deres synspunkter på innholdet i bestemmelsene og ønsker også synspunkter på om det er noe av dette som bør stå i forskrift av hensyn til forutberegnelighet for de som blir gjenstand for tilsyn.*

Vi er enige i departementets vurdering av at mye av innholdet i kapittel 4 kan, og muligens bør, ivaretas gjennom instruks.

Side 40: *Departementet ber om høringsinstansenes innspill til bestemmelsen, og vil vurdere behovet for ytterligere bestemmelser om eierskapskontroll i lys av høringsinstansenes innspill.*

Krav til eierskapskontroll må eventuelt vurderes i lys av konsesjonsordninger for produksjon av energi og petroleum.

Side 42: *Departementet ber særlig om høringsinstansenes innspill på denne innretningen for hvordan en virksomhet kan beskytte sine skjermingsverdige verdier på en slik måte at kravet til forsvarlig sikkerhetsnivå oppnås.*

Vi støtter denne tilnærmingen.

Side 42: *Departementet ber om høringsinstansenes syn på om definisjonene i bestemmelsen er nødvendig, og på om det er andre begreper som bør defineres.*

Vi har ikke funnet behov for andre definisjoner.

Side 44: *Det bør utarbeides veiledningsmateriale fra tilsynsmyndigheten eller sikkerhetsmyndigheten som kan brukes i vurderingen av hvilke roller som vil være tilstrekkelig i det enkelte tilfelle.*

Veiledningsmateriell bør utarbeides på generelt nivå. Sektorspesifikk implementering bør skje i samarbeid mellom tilsynsmyndigheten og de aktuelle virksomhetene.

Side 46: *Departementet ber om høringsinstansenes syn på bruken av begrepet «sikkerhetstruende virksomhet».*

Begrepet er definert i sikkerhetsloven som «tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser» og er et godt samlebegrep, samtidig som det synes uheldig at loven og underliggende forskrifter bruker virksomhetsbegrepet på to ulike måter.

Side 47: *Vi ber særlig om høringsinstansenes syn på denne innretningen. Departementet vil vurdere hensiktsmessigheten og utformingen av denne bestemmelsen.*

Det synes logisk å stille krav om at risiko ikke bare skal vurderes, men også håndteres. Samtidig kan vel i alle fall §§ 13 og 14 anses som verktøy til bruk for håndtering av risiko, og § 12 kunne derfor muligens vært brukt som et tydeligere bindeledd mellom krav til vurderinger og tiltak.

Side 50: *En evaluering av produkter eller tjenester må gjøres av en uavhengig tredjepart med nødvendig kompetanse.*

Det er på nåværende tidspunkt tilgjengelig kun et svært begrenset utvalg IEC 62443-sertifiserte produkter. Kravet i virksomhetsforskriften § 15 bokstav c kan bli krevende å implementere i eksisterende objekter og infrastruktur.

Side 64: *Departementet ber om innspill på om godkjenningsbestemmelsen er hensiktsmessig utformet.*

Vi har ingen merknader til utforming av § 48, men vi er enige i utgangspunktet i § 47 om at sikkerhetsmyndigheten er godkjenningsinstans i de tilfellene virksomheten selv ikke kan godkjenne.

Side 78: *Departementet ønsker høringsinstansenes innspill på hvordan plikten til å gi egenopplysninger bør reguleres.*

Vår vurdering er at dette punktet ikke trenger ytterligere presisering, annet enn den detaljerte listen om kriterier for sikkerhetsmessig skikkethet som framkommer av loven § 8-4.

Side 81: *Departementet ber om høringsinstansenes innspill på bestemmelsen, herunder om momentene i tilknytningsvurderingen bør fremgå tydeligere av forskriftene.*

Vi anser at NSM fortsatt bør utarbeider konkrete personellsikkerhetsmessige vurderinger av andre stater som foreslått i forskriften.

∞

Vi håper kommentarene kommer til nytte i avslutningen av forskriftsarbeidet. Dersom noe er uklart, eller det er ønskelig å diskutere videre med oss, ber vi dere ta kontakt for å avtale et møtetidspunkt.

Med hilsen

Finn Carlsen e.f.
fagdirektør

Hilda Kjeldstad
leder for regelverksutvikling

Dette brevet er godkjent elektronisk i Petroleumstilsynet og har derfor ingen signatur

Kopi:
Arbeids- og sosialdepartementet Postboks 8019 Dep 0030 OSLO